UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/760,556 | 01/21/2004 | Eui-hyeon Hwang | 1793.1185 | 8648 |

21171 7590 05/17/2006

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

| EXAMINER | |
|---|---|
| AU, SCOTT D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2612 | |

DATE MAILED: 05/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/760,556 | HWANG ET AL. | |
| | Examiner | Art Unit | |
| | Scott Au | 2612 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-3*~~4~~*5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3*~~4~~*5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

The application of Hwang et al. for a "User authentication method and apparatus" filed January 21, 2004 has been examined.

Claims 1-34 are pending.

### *Claim Rejections - 35 USC § 102*

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-3, 5-7, 11-12, 23-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Kawan et al. (US# 7,039,812).

Referring to claim 1, Kawan et al. disclose a user authentication method that authenticates a user based on a password input by the user and the user's biometrics information (col. 4 lines 40-51), the user authentication method comprising: determining whether a password has been input; setting a first threshold value if the input password matches with a registered password and setting a second threshold value if the input password does not match with the registered password; and determining whether to authenticate the user based on a comparison of the user's biometrics information with registered biometrics information and the first or second threshold value (col. 8 lines 28-38 and col. 9 lines 46-64).

Referring to claim 11, Kawan et al. disclose a user authentication apparatus that authenticates a user based on a password input by the user and the user's biometrics information (col. 4 lines 40-51), the user authentication apparatus comprising: a password input unit which determines whether a password has been input (col. 8 lines 29-38); a storage unit which stores a registered password and registered biometrics information(col. 10 lines 1-12); a threshold value setting unit which sets a first threshold value if the input password matches with a registered password and sets a second threshold value if the input password does not match with the registered password; and a biometrics unit which obtains biometrics information from the user outside, determines how much the obtained biometrics information matches with the registered biometrics information, and authenticates a user if the extent to which the obtained biometrics information matches with the registered biometrics information is larger than the first or second threshold value (col. 4 lines 40-51 and col. 9 lines 46-64).

Referring to claims 2 and 12, Kawan et al. disclose the method of claims 1 and 11, wherein the first threshold value is set so that a false rejection rate (FRR) is reduced and the second threshold value is set so that a false acceptance rate (FAR) is reduced (col. 9 lines 46-64).

Referring to claim 3, Kawan et al. disclose the method of claim 1, further comprising: storing a password input history (col. 10 lines 1-12); and it is inherent that

Kawan et al. suggest determining whether there has been an intrusion, by referring to the password input history if the user is not authenticated.

Referring to claim 5, Kawan et al. disclose the method of claim 1, further comprising: storing a password input history; and varying the first and second threshold values based on the password input history if the user is not authenticated (col. 10 lines 1-12 and see Abstract).

Referring to claim 6, Kawan et al. disclose the method of claim 5, wherein the varying the first and second threshold values, comprises varying the first and second threshold values so as to enhance a level of security if a wrong password is input at least n times (col. 2 lines 41-54).

Referring to claim 7, Kawan et al. disclose the method of claim 6, wherein the varying the first and second threshold values, comprises restoring the varied first and second threshold values if a correct password is input at least m times after the first and second threshold values are varied so as to enhance the level of security (col. 2 lines 41-54 and col. 9 lines 47-64).

Referring to claim 23, Kawan et al. disclose a computer-readable recording medium on which a program enabling the user authentication method of claim 1 is recorded (col. 10 lines 1-12).

Referring to claim 24, Kawan et al. disclose a user authentication method, comprising: adjusting a threshold level of a biometrics device which reads a user's biometric information based on a password input by a user, wherein the threshold level is broadened when the user inputs a valid password to increase the possibility of the user being authenticated by the biometrics device, and the threshold level is narrowed when the user inputs an invalid password to decrease the possibility of the user being authenticated by the biometrics device (col. 4 lines 40-51, col. 8 lines 28-38 and col. 9 lines 46-64).

Referring to claim 25, Kawan et al. disclose the method of claim 24, further comprising: comparing the user input password with a predetermined password, wherein when the user input password is valid, the user input password matches the predetermined password, a first threshold level which reduces a false rejection rate is set, and when the user input password is invalid, the user input password does not match the predetermined password, a second threshold level which reduces a false acceptance rate is set (col. 4 lines 40-51, col. 8 lines 28-38 and col. 9 lines 46-64).

Claims 24-26, and 33-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Sime (US# 5,386,104).

Referring to claim 24, Sime discloses a user authentication method, comprising: adjusting a threshold level of a biometrics device which reads a user's biometric information based on a password input by a user, wherein the threshold level is broadened when the user inputs a valid password to increase the possibility of the user being authenticated by the biometrics device, and the threshold level is narrowed when the user inputs an invalid password to decrease the possibility of the user being authenticated by the biometrics device (col. 4 lines 45-65).

Referring to claim 25, Sime discloses the method of claim 24, further comprising: comparing the user input password with a predetermined password, wherein when the user input password is valid, the user input password matches the predetermined password, a first threshold level which reduces a false rejection rate is set, and when the user input password is invalid, the user input password does not match the predetermined password, a second threshold level which reduces a false acceptance rate is set (col. 4 lines 45-65).

Referring to claim 26, Sime discloses the method of claim 24, wherein the threshold level is adjusted to incrementally reduce the possibility of the user being

authenticated by the biometrics device as a number of invalid password entries by the user increases (col. 4 lines 45-65).

Referring to claim 33, Sime discloses a user authentication method, comprising: authenticating a user by varying a threshold value of a biometrics device depending on whether a password input by the user matches a registered password (col. 5 lines 45-65).

Referring to claim 34, Sime discloses method of claim 33, wherein the threshold value comprises a first threshold value when the password input by the user matches the registered password and a second threshold value when the password input by the user does not match the registered password (col. 5 lines 45-65).

Referring to claim 35, Sime discloses method of claim 33, further comprising: varying the first and second threshold values to enhance a level of security when an incorrect password has been entered a predetermined number of times.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawan et al. (US# 7,039, 812) as applied to claims 3 and 11 above, and further in view of Saito et al. (US# 6,980,672).

Referring to claim 4, Kawan et al. disclose the method of claim 3. However, Kawan et al. did not explicitly disclose further comprising: storing an intruder's biometrics information upon determining that there has been an intrusion, wherein the determining whether there has been an intrusion, comprises authenticating the user based on a result of comparing the user's biometrics information with the intruder's biometrics information.

In the same field of endeavor of authentication system, Saito et al. suggest further comprising: storing an intruder's biometrics information upon determining that there has been an intrusion, wherein the determining whether there has been an intrusion, comprises authenticating the user based on a result of comparing the user's biometrics information with the intruder's biometrics information (col. 14 lines 26-35).

One ordinary skill in the art understands that storing intruder's biometric data of Saito et al. is desirable in the authentication system of Kawan et al. because Kawan et al. suggest the authentication system using the biometric data and the input PIN together (col. 4 lines 40-51) and Saito et al. suggest the authentication system using

the biometric data and storing the intruded biometric data in order to deter the unauthorized of opening the door (col. 14 lines 26-35).

Referring to claim 13, Kawan et al. disclose the apparatus of claim 11. Kawan et al. suggest the used of both password (PIN) and biometric data for authentication. However, Kawan et al. did not explicitly disclose storing of the password input in the storage if the password is not authenticated.

In the same field of endeavor of authentication system, Saito et al. suggest storing the biometric data of the intruder if the system is not authenticated (col. 14 lines 27-36).

One ordinary skill in the art understands storing the biometric data of the intruder if the system is not authenticated can alter biometric data into input password of Saito et al. is desirable in the authentication system of Kawan et al. because Kawan et al. suggest the authentication system using the biometric data and the input PIN together (col. 4 lines 40-51) and Saito et al. suggest the authentication system using the input data and storing the intruded input data in order to deter the unauthorized of opening the door (col. 14 lines 26-35).

Referring to claim 14, Kawan et al. in view of Saito et al. disclose the apparatus of claim 13, wherein the storage unit stores a password input history, and the biometrics unit determines whether there has been an intrusion by referring to the

password input history stored in the storage unit if the user is not authenticated (col. 14 lines 26-35).

Referring to claim 15, Kawan et al. disclose the apparatus of claim 11, Saito et al. suggest wherein the storage unit stores an intruder's biometric data (col. 14 lines 26-35), and Kawan et al. suggest the authentication is based on the threshold of the input PIN and biometric data (col. 4 lines 40-51). Therefore, it is obvious that the combining of Kawan et al. and Saito et al. teach the threshold value setting unit varies the first and second threshold values based on the password input history if the user is not authenticated.

Claims 8-10,18-20 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawan et al. (US# 7,039, 812) as applied to claims1 and 24 above, and further in view of O'Connor et al. (US# 6,938,159).

Referring to claim 8, Kawan et al. disclose the method of claim 1. However, Kawan et al. did not explicitly disclose further comprising:
adding/updating an authentication key if the user is authenticated.

In the same field of endeavor of authentication system, O'Connor et al. disclose adding/updating an authentication key if the user is authenticated (col. 6 line 61 to col. 7 line 8).

One ordinary skill in the art understands that adding/updating an authentication key if the user is authenticated of O'Connor et al. is desirable in the authentication system of Kawan et al. because both Kawan et al. and O'Connor et al. suggest biometric data is used for authentication (Kawan et al. and O'Connor, see Abstract) and O'Connor et al. suggest adding/updating an authentication key if the user is authenticated in order to establish and create a new identity reference.

Referring to claim 9, Kawan et al. in view of O'Connor et al. suggest the method of claim 8, O'Connor et al. suggest wherein the adding/updating the authentication key, comprises adding/updating the authentication key if the input password matches with the registered password and the user is authenticated by a biometrics unit (col. 6 line 61 to col. 7 line 8).

Referring to claim 10, Kawan et al. in view of O'Connor et al. suggest the method of claim 8, O'Connor et al. suggest wherein the adding/updating the authentication key, comprises adding/updating the authentication key if the user is authenticated (col. 6 line 61 to col. 7 line 8) and Kawan et al. suggest authentication by the biometrics unit and the extent to which the input password matches with the registered password is larger than a predetermined third threshold value (col. 4 lines 40-51, col. 8 lines 28-38 and col. 9 lines 46-64.

Referring to claim 31, Kawan et al. disclose the method of claim 24, Saito et al. disclose further wherein the updating the authentication key occurs only when the

password is valid and the level which the user's biometric information matches the authorized user's biometric information exceeds an updating authentication threshold (col. 6 line 61 to col. 7 line 8).

Referring to claim 32, Kawan et al. in view of Saito et al. disclose the method of claim 31, Kawan et al. disclose wherein the updating the authentication key occurs only when the password is valid and the level which the user's biometric information matches the authorized user's biometric information exceeds an updating authentication threshold (col. 4 lines 40-51, col. 8 lines 28-38 and col. 9 lines 46-64).

Referring to claims 18-20, Kawan et al. in view of O'Connor disclose an apparatus in claim 11, claims 18-20 are equivalent to that of claim 8-10 addressed above, incorporated herein. Therefore, claims 18-20 are **rejected for same reasons given with respected** to claims 18-20.

Claims 16-17,21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kawan et al. (US# 7,039, 812) in view of Saito et al. (US# 6,980,672) as applied to claim 15 above, and further in view of Sime (US# 5,386,104).

Referring to claim 16, Kawan et al. in view of Saito et al. disclose the apparatus of claim 15. Kawan et al. disclose the threshold can be adjusted to a high or a low level base on the biometric template in order to access the secure control at a desire level of control (col. 9 lines 50-64). However, Kawan et al. in view of Saito et al. did not explicitly disclose the level of security enhanced is based on the incorrect password is input n times or more.

In the same field of endeavor authentication system, Sime teaches the level of security enhanced is based on the incorrect password is input n times or more (col. 5 lines 45-65).

One ordinary skill in the art understands that the level of security enhanced is based on the incorrect password is input n times or more of Sime is desirable in the authentication system of Kawan et al. in view of Saito et al. because Kawan et al. and Sime teach using both the biometric data and input PIN to authenticate the system, and Sime teaches the counts of time the user attempt to access the system that providing alert when the count has not reached the threshold values.

Referring to claim 17, Kawan et al. in view of Saito and Sime disclose the apparatus of claim 15, Sime teaches wherein the threshold value setting unit restores

the varied first and second threshold values if a correct password is input m times or more (col. 5 lines 45-65).

Referring to claims 21, Kawan et al. disclose an apparatus in claim 11, claim 21 is equivalent to that of claim 16 addressed above, incorporated herein. Therefore, claim 21 is **rejected for same reasons given with respected** to claim 16.

Referring to claim 22, Kawan et al. in view of Saito and Sime disclose the apparatus of claim 16 above, Sime teaches a counter which counts the number of times an incorrect password is input (col. 5 lines 45-64), Saito et al. teach storing of a the detected biometric data in the authentication system (col. 14 lines 27-36). Therefore, it is obvious one skill in the art understand that the combination of Kawan et al. in view of Saito et al. and further Sime teach wherein the storage unit stores the obtained biometrics information output from the biometrics unit depending on the result of the counting in order to obtain a higher level of security.

Claims 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sime (US# 5,386,104) as applied to claim 26 above, and further in view of Saito et al. (US# 6,980,972).

Referring to claim 27, Sime discloses the method of claim 26. However, Sime did not explicitly disclose storing the user's biometric information as an intruder

biometric entry when the number of invalid password entries by the user equals a predetermined number.

In the same field of endeavor of authentication system, Saito et al. suggest storing the user's biometric information as an intruder biometric entry when the number of invalid password entries by the user equals a predetermined number (col. 14 lines 27-36).

One ordinary skill in the art understands storing the user's biometric information as an intruder biometric entry when the number of invalid password entries by the user equals a predetermined number of Saito et al. is desirable in the authentication system of Sime because Sime suggests the authentication system using the biometric data and the input PIN together (col. 4 lines 40-51) and Saito et al. suggest storing the user's biometric information as an intruder biometric entry when the number of invalid password entries by the user equals a predetermined number in order to deter the unauthorized of opening the door (col. 14 lines 26-35).

Referring to claim 28, Sime in view of Saito et al. disclose the method of claim 27, Sime discloses further comprising: comparing a subsequent user's biometric information with the intruder biometric entry, wherein when the subsequent user's biometric information matches the intruder biometric entry based on the threshold level set, the subsequent user is blocked from being authenticated (col. 5 lines 45-65).

Referring to claim 29, Sime in view of Saito et al. disclose the method of claim 26, Saito et al. disclose further comprising: storing the password input by the user as a password history; and storing the user's biometric information as an intruder biometric entry based on the password history (col. 14 lines 26-35).

Referring to claim 30, Kawan et al. in view of Saito et al. disclose the method in claim 29, claim 30 is equivalent to that of claim 28 addressed above, incorporated herein. Therefore, claim 30 is **rejected for same reasons given with respected** to claim 28.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Pu et al. (US# 5,933,515) disclose the user identification through sequential input of fingerprints.

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (571) 272-3063. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Hofsass can be reached at (571) 272-2981. The fax phone numbers for the organization where this application or proceeding is assigned are (571)-272-1817.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-3050.

Scott Au

SA
5/15/06

JEFFERY HOFSASS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600